ADVOKATSKA KOMORA VOJVODINE
Zmaj Jovina 20/1, 21000 Novi Sad
Tel/Faks:+381 (0) 21 529 459;+381 (0) 21 521 235
E-mail:akvojvodine@gmail.com

Број: 982/20

П Р А В И Л Н И К

О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО – КОМУНИКАЦИОНОГ СИСТЕМА АДВОКАТСКЕ КОМОРЕ ВОЈВОДИНЕ

НОВИ САД

Управни одбор Адвокатске коморе Војводине, на основу члана 66 Закона о адвокатури, 10 став 1 и члана 76 Статута Адвокатске коморе Војводине, члана 8 Закона о информационој безбедности (Службени гласник РС 6/16), члана 2 и 3 Уредбе о ближем уређењу мера заштите информационо – комуникационих система од посебног значаја („Службени гласник РС“ 94/2016), на седници одржаној 28. 05. 2021. године донео је:

П Р А В И Л Н И К
О БЕЗБЕДНОСТИ ИНФОРМАЦИОНО – КОМУНИКАЦИОНИХ СИСТЕМА АДВОКАТСКЕ КОМОРЕ ВОЈВОДИНЕ

I. УВОДНЕ ОДРЕДБЕ

Члан 1.

Правилником о безбедности информационо – комуникационих система Адвокатске коморе Војводине (у даљем тексту: Правилник) се ближе дефинишу и утврђују мере заштите информационо – комуникационих система (у даљем тексту: ИКТ систем), а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења, дужности и одговорности корисника информатичких ресурса Адвокатске коморе Војводине (у даљем тексту: Комора).

Члан 2.

Циљеви доношења Правилника су:

1. Прописивање процедура коришћења и заштите информационо – комуникационих система Коморе;
2. Прописивање овлашћења и одговорности запослених у вези са приступањем, коришћењем и у вези са безбедношћу и ресурсима ИКТ система;
3. Минимизација безбедносних ризика на начин да се спречи настанак и ублаже последице инцидената којима се угрожава или нарушава информациона безбедност;
4. Подизање нивоа опште свести, а посебно запослених у Стручној служби Коморе (у даљем тексту: Служба) о ризицима и опасностима које су везане за коришћење информационих технологија;
5. Унапређење и развој одговарајућих безбедносних апликација и обезбеђивање сталне контроле свих компоненти информационо – комуникационих система;
6. Складиштење и чување података на начин који обезбеђује приступ истима само од стране овлашћених лица;
7. Свеукупно унапређење информационе безбедности и провера усклађености примене мера заштите.

Члан 3.

Мере заштите ИКТ система, овлашћења и одговорности запослених у вези са приступањем, коришћењем и безбедности података и ресурса ИКТ система служе

превенцији од настанка инцидената и минимизацији штете од евентуалних инцидената и њихова примена је обавезна за све запослене.

Запослени у Служби Коморе морају бити упознати са садржином овог Правилника и дужни су да поступају у складу са Законом о заштити података о личности и овим Правилником, као и са процедурама које регулишу приступање, коришћење, безбедност и ресурсе ИКТ система.

Члан 4.

Запослени у Служби Коморе су дужни да приступају инфромацијама и ресурсима ИКТ система само ради обављања редовних радних задатака и да редовно и благовремено информишу овлашћено лице о свим сигурносним инцидентима и проблемима.

Непоштовање одредби овог Правилника, као и свако угрожавање или нарушавање информационе безбедности, повлачи дисциплинску одговорност запосленог.

Члан 5.

Мере заштите ИКТ система се односе на електронске комуникационе мреже, електронске уређаје на којима се чува и врши обрада података коришћењем рачунарског програма, оперативне и апликативне рачунарске програме, програмски кôд, податке који се чувају, обрађују, претражују или преносе помоћу електронских уређаја, организациону структуру путем које се управља ИКТ системом, корисничке налоге, тајне информације за проверу веродостојности, техничку и корисничку документацију, унутрашње опште акте и процедуре.

Члан 6.

Адвокатска комора Војводине врши јавна овлашћења у складу са одредбом члана 65 Закона о адвокатури и ради обављања послова из своје надлежности прикупља, обрађује, користи за потребе одлучивања у управном поступку о статусним питањима адвоката и адвокатских ортачких друштава и чува податке који су заштићени Законом о заштити података о личности.

Члан 7.

Поједини термини који се користе у функционисању ИКТ система имају следеће значење:

1) Информационо – телекомуникациони систем (ИКТ систем) је технолошко организациона целина која обухвата:
   а) Електроноске комуникационе мреже у смислу закона који уређује електронске комуникације,
   б) Уређаје или групе међусобно повезаних уређаја, таквих да се у оквиру уређаја, односно у оквиру барем једног из групе уређаја, врши аутоматска обрада података коришћењем рачунарског програма,
   в) Податке који се похрањују, обрађују, претражују или преносе помоћу средстава из подтачке а) и б) ове тачке у сврху њиховог рада, употребе, заштите и одржавања,
   г) организациону структуру путем које се управља ИКТ системом;
2) Информациона безбедност представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност, и непорецивост тих података да би тај систем функционисао како је предвиђено под контролом овлашћених лица;

3) Тајност је својство које значи да податак није доступан неовлашћеним лицима;

4) Интегритет значи очуваност изворног садржаја и комплетност података;

5) Расположивост је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;

6) Аутентичност је својство које значи да је могуће проверити и потврдити да је податак створио или послао онак за које је декларисано да је ту радњу извршио;

7) Непорецивост представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће поредити;

8) Ризик значи могућност наруштавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;

9) Управљање ризиком је систематичан скуп мера који укључује планирање,м организовање и усмеравање активности коко би се обезбедило да ризици остану у прописаним и прихватљивим оквирима;

10) Инцидент је унутрашња или спољна околности или догађај којим се угрожава или нарушава информациона безбедност;

11) Мере заштите ИКТ система су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;

12) Тајни податак је податак од интереса за Републику Србију који је законом, другим прописом или одлуком надлежног органа донесеним у складу са законом, одређен и означен одређеним степеном тајности;

13) ИКТ систем за рад са тајним подацима је ИКТ систем који је у складу са законом одређен за рад са тајним подацима;

14) Компромитујуће електромагнетно зрачење (КЕМЗ) представља ненамерне електромагнетне емисије приликом преноса, обраде, или чувања података чијим пријемом и анализом се може открити садржај тих података;

15) Криптобезбедност је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;

16) Криптозаштита је примена метода, мера и поступака ради трансформисања података у облика који их за одређено време или трајно чини недоступним неовлашћеним лицима;

17) Криптографски производ је софтвер или уређај путем кога се врши криптозаштита;

18) Криптоматеријали су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографски кључеви;

19) Безбедносна зона је простор у коме се, у складу са прописима о тајности података, обрађују и чувају тајни подаци;

20) Информациона добра обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компоненти, техничку и корисничку документацију, унутрашње правилнике, процедуре и слично;

21) Бекап је резервна копија података;